
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فاعلية

أزهري عبد الرحمن محمد خليل، عز الدين عثمان
جامعة السودان للعلوم والتكنولوجيا
الخرطوم، السودان
ص. ب 723، رمز بريدي 11111
izzedin@acm.orgazmoh65@gmail.com

نسرين بشير عثمان
كلية البيان للعلوم والتكنولوجيا
الخرطوم، السودان
ص. ب 210
nisreenbeshir@gmail.com

الملخص – تعني هذه الدراسة بتقديم معلومات أساسية للتكنولوجيا المحورية المستخدمة في عملية جمع وتوثيق وتحليل الأدلة الشرعية الرقمية وذلك لسد الحوجة الماسة لتوفير المعلومات الأساسية لتكنولوجيا التحقيق والسعي نحو الأسلوب الأمثل مباشرة التحقيق في الجريمة الإلكترونية ويشمل ذلك استعادة المعلومات المفقودة بتعمد من مرتكب الجريمة الإلكترونية أو نتيجة لمباشرة عملية جمع المعلومات، أو نتيجة للاستجابة الأساسية ضد المتعدي على النظام، وبرامج تقنيات مفاتيح الدخول، والأجهزة إلى جانب المتعلقات القانونية المعنية بعملية جمع الأدلة الرقمية، كما أن القصد من هذه الدراسة هو أن تكون مصدراً مختصراً وتقديماً وليس بديلاً لما هو متوفر من مصادر في هذا الخصوص بهدف الوصول إلى قواعد وموجهات عامة للمحقق عند استشراف عملية التحقيق في الجريمة الإلكترونية.

الكلمات المفتاحية — التحقق: الأدلة الشرعية الرقمية؛ الجريمة الإلكترونية؛ جمع الأدلة، التوثيق، قواعد وموجهات عامة.

1- مقدمة

تعني هذه الدراسة بتقديم المصدر أو المرجع المختصر لعملية التحقيق في الجرائم الإلكترونية وليس البديل لما هو متوفر من مصادر في هذا الخصوص وذلك من خلال استعراض (Presentation) وسائل جمع الأدلة الجنائية واستعراض الخلفية والخطوات الأمثل حتى الآن لمباشرة (Approach) التحقيق ووسائل التحقيق والتحليل في نظامي وندوز (Windows) ويونكس (Unix) وتطبيقات (Applications) طرق وخطوات استخدام تكنولوجيا حماية الأنظمة واسترجاع المعلومات (Restoration) من خلال استعراض (Presentation) كيفية التعامل مع الاعتداء (Infringement) والحصول على بقايا المعلومات (Data Remains) الممغنطة، ومراجعة سجلات الأنظمة (Systems Logs) إلى غير ذلك من تطبيقات وطرق وخطوات. وفوق ذلك استنباط موجهات فنية وقانونية يسير على هديها الموكل لهم النهوض بعملية مكافحة الجريمة الإلكترونية (Cybercrime Fighters) وقد كان هذا هو أهم أهداف هذه الدراسة التي ركزت على حصر المحاولات الفنية والتكنولوجية المتوفرة حتى الآن في عملية جمع وتوثيق وتحليل الأدلة الرقمية لاستخدامها كموجهات عامة Guidelines لمباشرة التحقيق (Investigation) في الجريمة الإلكترونية (Cyber Crime).

تستهدف معالجة الأدلة الشرعية الرقمية جمع وفحص الأدلة الإلكترونية، وتقييم الأضرار التي لحقت بالكمبيوتر نتيجة للهجمات الإلكترونية، ويشمل ذلك العمل والسعي لاستعادة المعلومات المفقودة، التي تمكن من تقديم مرتكب الجريمة الإلكترونية للمحاكمة. ومع تزايد أهمية أمن الكمبيوتر وخطورة الجريمة الإلكترونية أصبح من الضروري لمحترفي الكمبيوتر التمتع بالفهم القانوني، وفهم التكنولوجيا التي تستخدم في جمع الأدلة الرقمية، وكل ما هو دائر حول المعلومات الأساسية المتعلقة بالتقنيات المستخدمة في هذا الإطار. ويشمل ذلك استرداد البيانات، والاستجابة الأساسية لأي متسلل (Intruder) على النظام، وكل ما يتعلق بتكنولوجيا برمجيات الدخول الرئيسية، والأجهزة، والجوانب القانونية، والأخلاقية لتكنولوجيا جمع الأدلة الشرعية الرقمية [1].

صارت مسألة توسيع فكرة سيادة القانون (Rule of Law) في فضاء السايبر، ذات أهمية حتمها القلق، ونشدان الثقة لدى القطاعات المتعاملة مع تكنولوجيا السايبر. ويشمل التوسع المشار إليه، قطاع الأعمال (حكومياً (Governmental) أو خاصاً

(Private) أو قطاع الأفراد، (Individuals) فإذا وضعنا في الاعتبار أن التوسع والتمدد الخاص بتكنولوجيا السايبر ما زال في بداياته، بمعنى أن هذه التكنولوجيا مازالت آفاقها مفتوحة دون حدود، في وقت ما زالت فيه الجريمة الإلكترونية تقع عملياً تبعه مقاومتها على المتضررين منها، فإنه تقع على المؤسسات أعباء الدفاع عن أنظمتها، وحماية معلوماتها من التعديات والهجوم (Attacks) الذي قد يقع عليها[2] .

ولما كان الردع القانوني ما زال بلا فاعلية يمكن الاعتداد بها، فإن جل المنظمات والقطاعات المعنية تعكف باجتهاد ملحوظ على تنشيط خططها الخاصة بأمن تكنولوجيا السايبر في وقت يظل فيه تفعيل الخطط الأمنية الخاصة، وتجاوز مشكلات التكنولوجيا، وتوفير الأمن، معترضاً بمشكلة أن أجهزة الدفاع دائماً ما تعتمد على وسائل معقدة ومكلفة لإنتاجها، واستمرار تشغيلها، وعليه فإن توفير الأمن يتطلب ابتداء توفير موارد كافية لزيادة تثقيف محسوبي الجهة طالبة التأمين وذلك للاطمئنان على أن أهداف الخطوات الأمنية قد تم استيعابها تماماً، قبل وضع خطط أوسع للتعامل مع للمعلومات، والبيانات حسب حساسيتها، ويشمل ذلك السجلات، والعمليات، وبرامج مكافحة الفيروسات، والجدران النارية، وأدوات كشف التسلل، واستخدام التوثيق والتشفير، وكل ما تعلق منها بالصناعة والتشغيل والبرمجة.

2- **جمع الأدلة الجنائية الرقمية**

اكتسب استخدام البينة الرقمية أهميته من أن المحاكم أصبحت تقبل تقديم البينة الرقمية للفصل في القضايا المعروضة أمامها استدعى ذلك القبول، توفر قوانين قادرة على معالجة قضايا السايبر الحالية، والمتوقعة. وحتم هذا القبول أيضاً التعاون البناء بين أهل الفكر القانوني، ومحترفي الكمبيوتر وتقانة المعلومات.

عموماً فإن بعض القائمين على تكنولوجيا السايبر وبسبب مصاعب التشغيل، وارتفاع تكاليفه، ذهبوا إلى التنازل عن درجات الأمان الأعلى، وذلك بعدم تفعيل أجهزة الدفاع والأمن بصورة مؤثرة، وتعطيل آلياته، مما أدى لتذايد الاهتمام بالحماية القانونية [3]، وفنياتها، خصوصاً في مجال جمع الأدلة الشرعية الرقمية، ومراحل التحقيق بوجه عام[4]، لذا اهتمت هذه الدراسة بتقديم المصدر المختصر، بهدف الوصول إلى قواعد، وموجهات عامة للمحقق، عند استشراف عملية التحقيق في الجريمة الإلكترونية.

3- **المنهجية**

الخلفية والخطوات الأمثل لمباشرة التحقيق في الجريمة الإلكترونية.

اعتمدت الدراسة تحديد الخطوات الأمثل قانونياً وتقنياً بهدف تقريب الشقة بين الجانبين بافتراض أن الخطوات القانونية في مجال مكافحة الجريمة الإلكترونية، تمضي متسارعة، بينما المبادئ التوجيهية مازالت تبارح مكانها. الأمر الذي يبين أن خطوات المكافحة تحتاج المزيد من البحث والتدقيق، للخروج بنموذج عام متفق عليه، يكون مواكباً لسرعة تطور الجريمة الإلكترونية، ليكبح جماحها، ويخفف الرعب الذي تسببه.

4- **النتائج**

عند استشراف عملية التحقيق بواسطة الشرطة لابد من دفع المحققين لتبني المصادر المتعددة لقواعد وموجهات التحقيق، ومراعاتها، وهي تتمثل بشكل عام في المصادر التالية[5]:

* القانون الوطني (National Law) أو المحلي (Local Law) بمعنى مراعاة الإجراءات الجنائية (Criminal Procedures) واجبة الإتباع بنص القانون، أو القواعد القانونية الخاصة بطريقة جمع أدلة الجريمة الإلكترونية بما يوفر البينة محل التحقيق لأن البينة المقبولة لابد أن يتم الحصول عليها وفقاً للقانون وإلا أصبحت غير مقبولة.

* معايير وموجهات القانون الدولي (International Law): وأطره التقليدية والاتفاقيات والهيئات الدولية (كالبوليس الدولي Interpol) التي تعمل في إطار التعاون الدولي في مكافحة الجريمة الإلكترونية خاصة أو الجريمة عموما [6].

* المبادئ التوجيهية الكتيبات، (Principles, Guidelines and Manuals) التي تمد المحققين بالمرجعية التي تستند للتجربة العملية التي تساعد على اتخاذ القرار المناسب في الوقت المناسب مع شتى ضروب مراحل التحقيق.

خطوات جمع الأدلة الجنائية الإلكترونية

تشمل عملية جمع الأدلة الشرعية الإلكترونية الاحتفاظ، تحديد الهوية I، الاستخراج، التوثيق، وتفسير المعلومات المحرزة [7]. وهناك ثلاثة خطوات رئيسية في عملية جمع الأدلة الشرعية للجريمة الإلكترونية نتعرض لها في إيجاز فيما يلي:

تشمل عملية جمع الأدلة الشرعية الإلكترونية الاحتفاظ، تحديد الهوية، الاستخراج، التوثيق، وتفسير المعلومات المحرزة [8]. وهناك ثلاثة خطوات رئيسية في عملية جمع الأدلة الشرعية للجريمة الإلكترونية نتعرض لها في إيجاز فيما يلي:

أ- الاستحواز Acquiring : بالنسبة للأدلة الرقمية تحوي هذه الخطوة الاستحواز على المعلومات عن طريق خلق نسخة طبق الأصل (Replica) من المعلومات الموجودة بقرص التسجيل القرص الصلب (Hard disk) ولضمان الحصول على هذه النسخة (Copy) لابد من أن تكون عملية النسخ قد تمت بخطوات منتظمة شملت كل أجزاء القرص الصلب – bit – by bit الاختلاف بين خبراء الأدلة الجنائية يدور حول ما إذا كان أجدي قفل الجهاز مباشرة أم مباشرة جمع الأدلة بمجرد الضبط لتفادي خسران المعلومات الحساسة التي قد تتأثر بإغلاق الجهاز. الراجح إنه من الأفضل الحصول على نسخة طبق الأصل لضمان أن كل محتويات القرص الخاص بالمتهم تم الحصول عليها.

ب- التوثيق Authentication : وهو الاستيثاق من أن النسخة المستخدمة في عملية التحقيق هي نسخة طبق الأصل من محتويات النسخة الأصلية بالقرص الصلب. بمعنى أن النسخة الأصلية لم يحدث فيها أي تعديل أثناء عملية الاستحواذ لأن التعديل يؤدي إلى عدم قبول البينة أمام المحكمة.

ج- التحليل Analyzing : وهي خطوة تحليل المعلومات المحرزة والتي تقود بدورها إلى تجريم من ارتكب الفعل الإجرامي. وهي أكثر مراحل التحقيق استنزافاً للوقت.

5- المناقشة والاستنتاجات

مهمة المحقق هي معرفة أين يجد مخلفات الملفات المفقودة (Missed Files Remains) ويحلل نتائج المضبوطات، ولما كانت عملية التحليل هي الأهم في مراحل التحقيق ذهبت الدراسة للتعرض أولاً لعملية تحليل المعلومات في نظامي وندوز ويونكس بشيء من التفريد، لسببين أولهما أنهما الأكثر استخداماً وثانيهما أهمية فهم المحقق لما يجري فيهما قبل استشراف عملية التحقيق[9].

6- تحليل الأدلة الجنائية في نظام وندوز

بالرغم من أي عيوب يمكن تعدادها وهي في غير صالح نظام الوندوز إلا أن ذلك لا يغير في كونه الأكثر استخداماً كنظام تشغيل للكمبيوتر، لذا فإن أي محقق لابد من أن يكون ملماً بكيفية عمل هذا النظام وخصوصياته حتى يكون قادراً على إجراء تحقيق بنتائج يعتد بها. وتبدأ أساسيات هذه المعرفة من معرفة تخصيص أماكن الملفات إلى عملية مسح الملفات وهو أمر تقتضيه عملية استرجاع الملفات الممسوحة.

الوندوز NT والوندوز 2000 والإصدارات الأعلى تستخدم نظام الفايلات [10] (Files System) وهو نظام يحتفظ بسمات الملفات في ملف يسمى (MFT) والسمات الأكثر أهمية في هذا الملف بالنسبة للمحقق هي MAC TIMES وهو الملف الذي يحتفظ بالتاريخ والزمن الذي تم فيه التعديل والدخول أو خلق الملف، والبيانات ومكان المعلومات في القرص مع الملفات كما أن سمات أخرى كالفهارس (Indexes) يجب أن تحظى هي الأخرى باهتمام المحقق في ملف. MFT

في ملفات NTFS تكتب البيانات على القرص في شكل قطع ملتصقة تسمى عناقيد (Nodes) بأحجام تتحكم فيها المساحة المقتطعة من القرص وإصداره الوندوز (Widows Version) ويستخدم في ذلك ملفات BITMAP $ لمتابعة العناقيد في القرص وهذا الملف يستخدم للإفادة عن تخصيص موقع للعناقيد بالقرص.

فعندما يخصص الموقع يتم خلق سجل بال – MFT (Master File Table) ورقم فهرست (Index Number)، وعندما يتم حزف الملف من مكان المتابعة BITMAP $ ويرقم ال BIT صفرا ويعلم ال MFT للمسح يرفع الفهرست إلى أعلى للمسح ولكن في حالة أن الدخول قد جاء الأخير فإن معلومات الدخول تظل مرئية ويكون ممكناً استرجاع سمات الملف (File Attributes) التي قد تتضمن زمن الدخول (Login Time) ومعلومات أخرى مفيدة في التحقيق، يقوم ال NTFS باستبدال السجلات الممسوحة (Deleted Files) لخلق سجل جديد لذا فإن الاستبدال لا يتم فتكون سمات الملف موجودة في ذات الحين وربما استرجاع المعلومات (Information Restoration) أيضاً، وفي أحيان أخرى يكون ممكناً استرجاع المعلومات حتى بعد الاستبدال (Replacement) في MFT وفهرست الملف الأساسي [11] فإن كانت المعلومات كبيرة بما يكفي فإنها تستقر بأحد العناقيد بدلاً عن MFT نفسه، والعناقيد الحاوية للملفات الممسوحة تستقر بالتالي بالمساحات غير المخصصة وهذه بدورها يحتاج الوصول إليها استخدام أدوات التحقيق وهذا يدفع للقول بأهمية البحث في المساحات غير المخصصة فربما لم يحدث فيها استبدال بعد، خلافاً للفهارس الخاصة بالملفات المزالة.

يمكن للمحقق أيضاً مقارنة الملفات المعاد تسميتها (Renamed) بالملفات الممسوحة وبانطباقها يكون قد حصل على دليل بعلم المتهم بوجودها إذا كان هو من قام بتحويلها، كما أن MAC تفيد علم المتهم عندما تؤكد أزمان الخلق (Creation) والتعديل (Change) وآخر دخول.

يمكن للمحقق تفتيش ال ملف INFO للحصول على معلومات تخص الملف المعين وهي معلومات مفيدة كالمكان السابق للملف والاسم الأصلي وتأريخ المسح وهي معلومات قد تفيد ربط المتهم بأي فعل.

مناطق أخرى عديدة لابد من اعتبارها عند البحث كالمنطقة بين العناقيد التي قد تحوي بقايا ملفات ممسوحة وتسمي بملفات الركود (Slack Files) وتزيد مع كبر العناقيد. ومساحات المبادلة لابد أيضاً من اعتبارها في البحث فهي قد تحوي بقايا هامة لملفات ممسوحة قريباً لتستقر في مكان خاص في مساحة المبادلة (Swap Files) وعندما لا يكون هناك مجال لاستقرارها في ال RAM يحولها نظام التشغيل OS إلى مساحة المبادلة.

كما يمكن للمحقق البحث في ملفات الإنترنت المحفوظة مؤقتاً Index. DAT التي تحتوي عناوين URL وتأريخ آخر تعديل أو دخول ومثلما يمكن مسح هذه الملفات فإنه يمكن استرجاعها في المواقع الأخرى التي تم ذكرها [12].

إلى جانب البحث في سجل البرنامج للحصول على الدليل فإن المحقق يمكنه استخدام مصدر آخر لاسترجاع الملفات والحصول على الدليل وهو NTFS $ LOGFLE الذي يمكن المحقق من الحصول على كل العمليات التي تمت في NTFS كما أن هذا الملف يستخدم لما بعد انهيار النظام. من هذا الاستعراض الخاص بنظام الوندوز يمكن القول أن النظام يتيح مصادر عديدة ومفيدة للحصول على معلومات متنوعة تمكنه من إثبات الجرم وهي مصادر تفوق ما تم ذكره من أمثله.

7- تحليل الأدلة الجنائية في نظام يونكس

استشراف التحقيق في نظام يونكس يماثل كثيراً مباشرته في نظام الوندوز إذ يلزم المحقق الإلمام بكيف يخصص النظام المساحات، وكيف يقوم بمسح الملفات للوصول للملفات المخبأة (Hidden Files) أو الممسوحة في حين أنه يجب القول أن خصائص اليونكس تمنح المحقق فرصاً أفضل وأكثر تعدداً منها في نظام الوندوز.

فالاختلاف بين النظامين تمحور في مفاهيم التعامل مع الملفات إذ بعد أن تعرضنا لتعاملات الوندوز فيجدر ذكر أن اليونكس يستخدم مفهوم العقد أو نقاط التلاقي (Terminals) لتمثيل الملف وكل يحوي مؤشرات للمعلومات الفعلية في القرص مما يشكل معلومة مفيدة للمحقق فهي تحوي هوية المالك وأذن الدخول) كل الصلاحيات (Roles) وأرقام الدلائل المرجعية (Directory Numbers)، وال MAC وأحجام

الملفات (File Size) مع ملاحظة أن أسماء الملفات يتم تخزينها كمدخل في الدالة مع موقع نقطة التلاقي أو العقدة كما تجدر الإشارة إلى أن اليونكس يخصص المساحات للملفات في كتل (Blocks) أو قطع موازية لل NTFS في الوندوز وبالمثل يمكن البحث عن بقايا الملفات والسمات بين القطاعات أو الكتل Blocks لذات الاحتمال الذي يتم البحث بسببه في الوندوز بين ال NTFS.

مسح الملفات في اليونكس يتضمن الإشارة إلى اسم الملف في الدالة (Function) كغير مستخدم (Unused) ويؤدي ذلك لفقدان الصلة بين اسم الملف وملف البيانات الفعلية وسمات الملف والتأشير على الملف بغير مستخدم مع فقدان بعض السمات وليس جميعها ويشمل التأشير بغير مستخدم كتلة البيانات (Data Block).

وفقاً لأدوات التحقيق (TCT) في ملفات المعلومات وسماتها فإن الملفات الممسوحة في نظام يونكس تبقى لفترة طويلة في الأنظمة المستخدمة بكثافة لأن نظام الملفات في يونكس مرتبط ببعضه ولا يخلي المساحات بصورة عشوائية الأمر الذي يبقى الملفات الممسوحة لزمن أطول بافتراض أن الملفات الجديدة لا تتطلب ذات المساحات الخاصة بالملفات الممسوحة وهذه الخاصية تتيح الفرصة لاستعادة الملفات أفضل مما هو عليه الحال في نظام الوندوز وبالتالي فإن فرص المحقق في الحصول على ما يحتاجه تظل أفضل باستخدام كورونرس تولس (Coroners Tools) وأخرى تساعد في استعادة الملفات مثل Unrum إضافة لاستعادة السمات باستخدام Ils Tools المتوفرة في ال TCT وهي أجزاء هامة للمحقق خصوصاً عند مراجعة ال MAC time لأي ملف وتأتي الأهمية من أن المحقق يحتاج تحديدها لمعرفة التغيير الذي يحدث في الملفات المتصلة بها علماً بأن المعلومات في نظام اليونكس تحفظ في شكل ملفات (Files) وبالتالي فإن أي تغيير قد يثبت علم المتهم بالتغيير الذي حدث [13].

تحتوي ال TCT على أداة تسمى Mactime تعرض ملفات ال MAC times التي يستطيع ذوي الخبرة من المجرمين تغييرها لإخفاء العقد لذا يجب تجنب الاعتماد كلية على MAC times.

اليونكس يمنح المحقق الفرصة لتكرار الأوامر المستخدمة في الجلسات السابقة لذا تحفظ الأوامر في ملفات تأريخية (History Files) محمية وهذه بدورها تخضع للتحليل لتتبع خطوات المجرم برغم قدرته على محو هذه الملفات التي لا تكون ذات فائدة للمحقق إلا لوقت محدود. عموماً يمكن أن نخلص إلى أن عملية استخلاص الأدلة في اليونكيس تشبه كثيراً العملية في الويندوز غير انه يمكن استخدام أدوات اليونكس لاستخلاص المعلومات للبحث في منظومات بعينها بفاعلية أكثر.

8- تطبيقات، طرق وخطوات استخدام تكنولوجيا حماية الأنظمة واسترجاع المعلومات

عطفاً على ما خلص إليه البحث فقد تنوعت محاولات حماية الأنظمة والمعلومات ونتيجة لتنامي مشكلة الجريمة الإلكترونية وتواتر الجهد الفني والتقني لتوفير أسلوب وأدوات تساعد على استرجاع البيانات المفقودة أو إثبات المسئولية عن الفعل المجرم وكشف كيفية ارتكاب التعدي على الأنظمة وزيادة فاعلية حمايتها وغير ذلك من أدوات كشف الجريمة الإلكترونية والتحقيق الجنائي، فقد خلصنا لأهمها وأكثرها استخداماً والتي تم الإجماع على أهمية دورها في مسألتي الحماية من الجريمة الإلكترونية والتحقيق بشكل نرى أن إلمام المحقق في الجريمة الإلكترونية بها يجب أن يعد أساسياً:

9- التعامل مع الاعتداء والحصول على بقايا المعلومات الممغنطة

المعلومات التي تم استبدالها في قرص الكمبيوتر الصلب يبدو أمر استرجاعها للوهلة الأولى غير ممكناً بإتباع الفنيات الخاصة بالاسترجاع الذي سبقت الإشارة إليها، إلا أن حقيقة أن القرص الصلب يتكون من كومة أو مجموعة من الأقراص المغطاة بمادة مغنطيسية تحفظ سلسلة من الواحد والصفر، التي تكون البيانات المكتوبة في مسارات القرص المغنطيسي (مجموعة مسارات دائرية ترتكز على مركز واحد (Concentric) وأنه عندما يتم استبدال المعلومة المكتوبة على المدار لا يمكن أن يكون التسجيل الجديد بالدقة التي تمكن من تغطية المعلومة القديمة فإنه يمكن عن طريق جهاز متخصص (Magnectic Force Microscopy) (MFM) استرجاع أجزاء المعلومة التي لم يغطيها الاستبدال [14] وبكفاءة عالية جداً – هذا النوع من استعادة المعلومات نادراً ما يستخدم بسبب التكاليف الباهظة للجهاز الذي ينجز العملية. كما أن كثير من مديري الأنظمة تكون ردة فعلهم خاطئة عند حدوث الاعتداء وذلك بإعادة تشغيل النظام بينما الأفضل هو التأكد من الحصول على صورة من حالة النظام التي يجب أن يتم تسجيلها بدقة قبل أن تتعرض ولو بالصدفة للتعديل وخلق نسخة دقيقة من محتويات الملف لأن الهجوم قد

يتكرر. لذا فإن الحصول على الدليل يجب أن يكون هو الهاجس مع نسخة من نظام الملفات وهذه النسخة يتم الحصول عليها باستخدام برامج تصوير القرص. وبعد الحصول على النسخة المطلوبة يجب الحفاظ على القرص الأصلي بصورة آمنة للاستخدام عند الضرورة القصوى وبالحد الأدنى.

10- سجلات الأنظمة وصيانة النظام

أكثر الأدلة فاعلية وتمكيناً للمحقق من ربط الوقائع هي سجلات الأنظمة (System Logs)، وكلا النظامين وندوز أو يونكس يستطيعان تسجيل الأحداث الهامة بتفاصيلها عند حدوثها مما يستدعي أن تكون في حالة تشغيل قبل حدوث التعدي لتكون صورة التعدي أكثر وضوحاً. ومن أكثر سجلات الأنظمة (System Log) فائدة هو سجل الدخول وسجل التوصيل (System Connection) وهذا السجل يعطي صورة واضحة لتأريخ وزمن الدخول والعنوان إلى جانب أي بداية للتحرك غير الطبيعي أو محاولة الدخول من عنوان غير معروف لموقع غير عادي. في حالة نجاح المعتدي والدخول فإن السجل يكون قادراً على الاحتفاظ بسجل أوامر تأريخي يفسر بصورة واضحة هدف المعتدي من دخول النظام والملفات التي تمكن من اقتحامها أو تغييرها. وقد تكون هناك بعض الصعوبات المتعلقة بالإجراءات التي مازالت في طور التنفيذ، إلا أن توقف الإجراء قد يتيح استخراج جدول الرموز والمحتويات الأساسية وإجراء التحليل عليها.

يترك المعتدين الكثير من الأدلة وكثيراً ما يتركون بعض البرامج والمعلومات في النظام المعتدي عليه وذلك غالباً لاستخدامها في الاعتداء على أنظمة أخرى، وتسمى بقايا ملفات (Files Remains) وقد تحوي أي شيء شامل الفيروسات لمزيد من التحطيم وغالباً ما يستبدلون البرامج القابلة للتنفيذ ببرامج معدلة من إخراجهم لها خصائص مدمرة لذا لابد من مراجعة الأنظمة بشكل منظم وإجراء اختباريات مثل (Master Digest 5) – (MD 5) أو (Secure Hash Algorith - 1) –(SHA - 1) في ملفات النظام وفي حالة حدوث أي طارئ يمكن إجراء المقارنة للتأكد من عدم حدوث أي عبث. ثم أن المتعدي قد يلجأ لإخفاء الملفات في مناطق غير متوقعة ومنحها أسماء غير مألوفة يصعب الوصول إليها إلا أن هذه الملفات المخفية يمكن الوصول إليها باستخدام الأدوات المناسبة المتوفرة كأدوات أو تقنية [15].

11- متابعة أدوات التلصص والوصول للمتلصص

بعد فحص السجل والقيام بالتفسير المناسب لنشاط المتعدي يكون الوقت قد حان لتتبع المجرم وهو أمر ليس بالهين. سجل النظام (System Log) هو الطريق الوحيد لمعرفة المسئول عن الهجوم، إذ جرت العادة أن يقوم المعتدون بتعديل أو مسح السجل الذي يساعد على تتبعهم لذا يفضل دائماً أعداد النظام ليقبل كتابة السجل في نظام معزول لمنع المعتدي من الدخول ويفضل تبني طريقة التشفير (Encryption) والاختبارية في ترتيبات النظام وتنفيذه وهذا أمر يضمن إمكانية استرجاع البيانات وربما القبض على المتعدي وتشمل هذه الإجراءات سجلات جهاز توجيه الشبكة لأن مجرد الوصول للعنوان يجعل الوصول إلى النظام في حكم المؤكد.

أدوات التلصص هي أدوات تعمل في الخفاء وهي قادرة على الاختفاء تماماً خصوصاً ما تحدثه من تعديل في إعدادات النظام، وقد تطورت هذه الأدوات لحد بعيد فقد أصبحت قادرة على تصوير كل ما يظهر أو يعرض على الشاشة من أحداث بأوقات محسوبة وهذه الأداة تتكون عادة من جزأين:

أ– مكتبة الارتباط الحيوية (DLL) الذي يختص بالتسجيل.

ب– (exe) الذي يتولى تحميل DLL وإيصال صنارة لوحة المفاتيح (Keyboard Hook).

الصنارة (Hook) يقصد بها التقنية التي تستخدم وظيفة لاعتراض (Intercept) أحداث قبل وصولها إلى برنامج ومن ثم يسيطر على لوحة المفاتيح قبل الوصول إلى البرنامج المعني [16].

تأتي الصنارة في صورتين الأولى تأتي على نطاق النظام والأخرى محددة الموضوع أما ال DLL فهي ملفات تحمل وظائف ومعلومات أخرى متصلة ببرنامج في وقت التشغيل فعندما يتصل ال DLL بالعمليات ويأخذ مكانه في مساحة عنوان العملية يكون من الممكن الاستدعاء من العملية ال DLL تستخدم صنارة لوحة المفاتيح لأن أي برنامج في هذه الحالة يستطيع استدعاء تسجيل الدخول منها وبالتالي تسجيل كل ما يحدث من كل البرامج.

يمكن توصيل برامج التلصص بصورة مباشرة أو عن بعد باستخدام برامج الفيروسات أو عن طريق متعدي لديه مدخل أساسي للنظام. برامج التلصص عادة ما تحتاج ذاكرة قليلة لا تؤثر على أداء النظام لذا فهي تبقى بدون أن تتم ملاحظتها أو الوصول إليها. هناك منتجات فاعلة ضد التطفل قادرة على الوصول للمتطفلين هذه البرامج تعمل باستثارة بحث الذاكرة وملاحظة البرامج التي تتصرف بشكل غير طبيعي منها برنامج يدعي كي باترول [17] وهي تستخدم خوارزميات للكشف عن السلوك وخوارزميات النمط المتطابق (Pattern – Matching Algorithms) يعمل هذا النوع من الأدوات على كشف برنامج التلصص بمجرد اتصاله بلوحة المفاتيح بكشف استدعاء إجراء لوظيفة (Procedure Call) لتلصص كما يمكن لهذه الأدوات تفتيش الذاكرة ومقارنة البرامج ببرامج التلصص العديدة مثل ما يحدث في برنامج مكافحة الفيروسات.

هناك خيار آخر لمراقبة برامج التلصص هو الخيار المادي والذي يتم بإيصال جهاز بلوحة المفاتيح وأشهرها هو كي قوست وهو جهاز صغير يلحق بنهاية وصلة لوحة المفاتيح ويثبت في الجزء الخلفي للكمبيوتر. هذا الجهاز يعمل مع كل أنظمة التشغيل، ولا يمكن كشفه ببرامج التطفل، ولا يحتاج أية خبرة لتركيبه ولا يشترط لتركيبه أن يكون الكمبيوتر في وضعية معينة، وهو مستقل عن نظام التشغيل.

عيوب هذا النظام أنه يحتفظ بمساحة تخزينية بين 128.000 – 2.000.000 وبمجرد امتلاك الذاكرة وقبل تفريغها يبدأ في الاستبدال والتسجيل فوق المادة الموجودة أصلاً، وعيب آخر هوانه يمكن ملاحظة وجود الجهاز المثبت في الجهاز.

12- الخاتمة والتوصيات

عمدت هذه الدراسة إلى الوصول لنتائجها، عبر استعراض أهم مشاكل جمع وتحليل وتوثيق الأدلة الخاصة بمكافحة الجريمة الإلكترونية ثم استعراض معلومات أساسية للتكنولوجيا (Information Survey) المحورية (Pivotal) المستخدمة في عملية (Process) جمع وتوثيق وتحليل الأدلة الشرعية الرقمية بقصد توفير المصدر المختصر (Brief Source) وليس البديل (Substitute) لما هو متوفر من مصادر في هذا الخصوص بهدف الوصول إلى قواعد (Manuals) وموجهات (Guidelines) عامة للمحقق عند استشراف عملية التحقيق في الجريمة الإلكترونية. (Cyber Crime) ومما توفر من معطيات المناقشة والاستنتاجات خلصت الدراسة إلى ما يلي من نتائج وتوصيات:

1- تنامت مشكلة الجريمة الإلكترونية، وتعددت محاولات مكافحتها من الناحية القانونية والناحية الفنية.

2- الناحية الفنية تتخلف عن الناحية القانونية في عدة وجوه فإن كانت الدول وخصوصاً العربية قد أصدرت عدداً لا بأس به من التشريعات فإن الناحية الفنية مازالت بعيدة عن الوصول بها إلى المستوى الفاعل في مكافحة الجريمة الإلكترونية.

3- من معوقات هذه الدراسة غياب المراجع وشح الإحصاءات العربية ومن ثم فإن المصادر والمراجع المستخدمة في هذه الدراسة لا تعكس الحال في العالم العربي وأن كانت تلقي بعض الضوء على ما يمكن مشرعاً لأن الأهم الآن هو الاهتمام بالبحث والتدريب وتأهيل الطاقم البشري للتصدي لمشكلة الجريمة الإلكترونية والاستعداد لها بالتأهيل البشري والتقني والقانوني.

4- لابد من استنباط موجهات فنية وقانونية يسير على هديها الموكل لهم النهوض بعملية مكافحة الجريمة الإلكترونية.

5- ركزت الدراسة على حصراهم المحاولات الفنية والتكنولوجية المتوفرة حتى الآن في عملية جمع وتوثيق وتحليل الأدلة الرقمية لاستخدامها كمرجع لا يغني عن المراجع الأخرى إلا أنه يسهم في خدمة مستخدمي اللغة العربية أكثر، مع توصيتنا بضرورة إعطاء أولوية للتدريب وتأهيل الطاقم البشري.

6- موازيا الاهتمام بالناحية التقنية فإن التحقيق في الجريمة الإلكترونية تعترضه مسألتان من مسائل الخصوصية لابد من وضعها في الاعتبار :

* ضرورة تجنب الوقوع في خطأ التفتيش وحيازة الأدلة دون سند قانوني.

* إن الإنترنت يعد منتدى عاما يوفر حرية الكلام وتوصيل صوت الألقية إلا أن هذه الحرية.

* محدودة بكونها لا تهدد أمن النظام ولا تدخل في توصيف أخر يصل لدرجة أنه قد يصدر عنها فعل يعد جريمة.

المراجع

1) Bob Sheldon. Forensic Analysis of Windows Systems, from Handbook of Computer Crime Investigation: Forensic Tools and Technology, ed. Eoghan Casey. Academic Press, Bath, England 2002
2) Hinduja, S. (2003).Trends and Patterns among Online Software Pirates, Ethics and Information Technology 5.
3) David Icove, Karl Seger & William VonStorch, Computer Crime,A Crimefighter's Handbook, 1st Edition August 1995, 2001, O'Reilly & Associates, Online Available at: http://oreilly.com/catalog/crime/chapter/cri_02.html
4) Rob van den Hoven van Genderen, Cybercrime investigation and the protection of personal data and privacy, 2008, Online Available at: http://www.coe.int/t/dghl/cooperation/economiccrime /cybercrime/documents/reports-presentations/567%20study5-d-provisional.pdf
5) Comprehensive Study on Cybercrime February 2013 UNITED NATIONS OFFICE ON DRUGS AND CRIME Vienna
6) Junsik Jang BEST PRACTICES IN CYBERCRIME INVESTIGATION IN THE REPUBLIC OF KOREA" Even without compulsory regulation, pursuing international legal references is considered desirable."
7) Warren G. Kruse II and Jay G. Heiser. Computer Forensics: Incident Response Essentials. Addison Wesley, Boston 2001
8) Technical Working Group for Electronic Crime Scene Investigation. Electronic Crime Scene Investigation: A Guide for First Responders, July 2001.
9) "A hex editor (or binary file editor or byte editor) is a type of computer program that allows for manipulation of the fundamental binary data that constitutes a computer file."http://en.wikipedia.org/wiki/Hex_editor
10) NTFS (New Technology File System) is a proprietary! file system developed by Microsoft. Starting with Windows NT 3.1, it is the default file system of Windows NT family. en.wikipedia.org/wiki/NTFS
11) Digital Evidence Collecting & Handling, March 20, | 2002. [Cited May 21, 2003]. http://faculty.ncwc.edu/toconnor/495/4951ect06.htm
12) Bob Sheldon. Forensic Analysis of Windows | Systems, from Handbook of Computer Crime Investigation: Forensic Tools and Technology, ed. Eoghan Casey. Academic Press, Bath, England 2002
13) Wietse Venema. File Recovery Techniques. Dr. Dobb's Journal, December 2000. [cited May 21,2003]. http://www.ddj .com/documents/s=878/ddj0012h/0012 h.htm.
14) Peter Gutmann. Secure Deletion of Data from Magnetic and Solid-State Memory, Sixth USENIX Security Symposium Proceedings, 1996.available at http://www.cs.quckland.ac.nz/~pgut001/pubs/secure_deLhtml.
15) Dan Farmer and Wietse Venema. Computer Forensics Analysis Class, August 1999. http://www.porcupine.org/forensics/handouts.html
16) University of Sydney, Australia. Byron S. Collie. Intrusion Investigation and Post-Intrusion Computer Forensic Analysis. September2000. http://www.usyd.edu.au/su/is/comms/security/intrusio n_investigation.html
17) PestPatrol,Inc. /http://research.pestpatrol.com/KeyPatrol

Keywords—Investigation; forensic; Cyber Crime; data collection; authentication; Manuals & Guidelines.